OSD Policy/Guidance for FY07
OMB A-11, Exhibits 53 and 300
And NDAA, Sec 332

General

1. Initiatives identified in attachment A must submit an Exhibit 300 and a Selected Capital Investment Report (SCIR). SCIR's are required for the President's Budget submission only. Additional guidance regarding timelines for the President's Budget submission will released from OASD(NII) in December 2005.

2. Performance-based Acquisition Management. Services and Defense agencies must follow present DoD guidance on Earned Value Management (EVM) dated March 7, 2005. DoD will conduct EVM on appropriate contracting vehicles as prescribed in present guidance. In addition, DoD does not require the EVM to be applied to government/internal resources.

3. Compliance with A-11 exhibits 53 and 300. DoD will complete the Exhibit 300 IAW the 99% solution and final schema released by OMB on May 26, 2005. If there is inconsistency with other guidance, the schema will supersede.

4. Units of measure. All dollars will be reported in the Exhibit 300 and SCIRs in dollars Millions, out to two decimals (e.g., $1,300,000 = 1.30). All dollars in the resources section of SNaP-IT will be reported in Thousands (e.g., $1,300,000 = 1,300).

5. Consolidated Business Case for Infrastructure. For the Budget Estimate Submission (BES), MILDEPs and DISA will provide consolidated business cases for infrastructure per the format provided as attachment B, as a Word document, due not later than August 29, 2005. MILDEPs and DISA will also provide a verbal brief to OMB sometime after the FY07 BES submission.

6. Consolidated Business Case for Enterprise Architecture. For BES, MILDEPs will provide a consolidated business cases for enterprise architecture per the format provided as attachment C, as a Word document, due not later than August 29, 2005. MILDEPs will also provide a verbal brief to OMB sometime after the FY07 BES submission.

7. Business Modernization Management Program: DoD Core Business Mission Areas will complete a modified Exhibit 300 per the format provided as attachment D, as a Word document, due not later than August 29, 2005. The Transition Support Office (TSO) will complete an Exhibit 300 for the TSO effort (Initiative No. 6497). All Core Business Mission and TSO resources are to be reported in the exhibit 53.

8. Configuration Control. The Select & Native Programming Information Technology (SNaP-IT) database, formerly Information Technology Management Application (ITMA), is the department's authoritative source for IT Budget information. SNaP-IT will be used

to collect all information required for the OMB exhibits and congressional IT Budget materials.

9. NSS Business Rules. The following categories within SNaP-IT are automatically identified as NSS. They are:

a. GIG Group items identified as "FAA-Functional Area Applications" with C2, Intel, Science and Technology or LOGISTICS _ WARFIGHTER identified as the GIG Value.
b. GIG Group items identified as "IAA-Information Assurance Activities" - All are categorized as NSS.
c. Secondary GIG Group items identified as "WF-WAR FIGHTER INFRASTRUCTURE" - All are categorized as NSS.
d. All others initiatives will be categorized as IT.

10. OMB requires self-assessment scores for all Exhibit 300s. For scoring, all exhibit 300s will lock on noon July 22, 2005 and self-assessment scoring will be conducted the week of July 25, 2005. Scoring for the BES submission will be without resource information. Scores and comments will be provided to Services/Agencies not later than August 12, 2005. Exhibit 300s should be revised as necessary before SNaP-IT locks on August 29, 2005. Categories on each Exhibit 300 that scored low (<3 in any category other than security; <4 for Security) during the first review will be scored again after SNaP-IT locks. The IT Budget sent to OMB will reflect the final scores for the Exhibit 300s forwarded to OMB for FY07 BES.

11. Statement of Compliance requirement: The following supersedes FMR Chapter 18, Section 180102(G) and will be incorporated in the next update of the FMR.

> "G. Statement of Compliance Requirement: The IT/NSS submissions are electronic transmissions, however, both the CIO and the CFO of the component must sign a joint or coordinated transmittal memo that states that the submissions are complete; accurately aligned with primary budget, program and/or acquisition materials; and are consistent with Clinger-Cohen, OMB Circular A-11 and documented exceptions to the Circular, DoD CIO budget guidance memorandum, Paperwork Reduction and other applicable Acts and requirements. Statement may be based on the Program Manager's statement of compliance. Statement should also include explanations for investments that do not conform to DoD CIO budget guidance memorandum. This statement of compliance must be provided *by February 14 of each year* for the final submission for the President's Budget Request submission. Submission provided by the due date for entry into the Select & Native Programming Information Technology (SNaP-IT) database will be treated and distributed as "preliminary". Additional fine-tuning of DoD and component overall budgets due to clean up actions and/or late breaking modifications can potentially alter the preliminary submission. Coordination and reconciliation with other budget exhibits must take place before final submission. To the greatest extent possible resource changes within the component budget, should net to zero between the preliminary and final submissions. Final submission requirements will be addressed

within the NII IT Budget Guidance memo."

A sample format for the Statement of Compliance is provided at attachment E. Submissions should be sent to Mr. Craig Garant via email at craig.garant@osd.mil or fax at 703-693-7036.

12. For initiatives required to submit the Exhibit 300 or requesting $10M or greater in FY07 funding, components must answer the explanation of change questions in SNaP-IT. Joint programs must consider all initiative funding sources. It is preferred the questions be completed by SNaP-IT lock (August 29, 2005), however, components will have until COB September 16, 2005 to complete the explanation of change questions for BES. Due date for PB is NLT February 14, 2006. Specifically,

a. By appropriation, CY to BY funding changes of plus or minus 25% must be explained.

b. By appropriation, FY06PB BY+1 (FY07 column of the FY06 PB) to FY07BES BY (FY07 column of the FY07 BES) funding changes of plus or minus 10% must be explained.

Clarification for FY07 reporting format

Exhibit 53

1. OMB and the DoD have made significant data collection changes since submission of the FY 2006 President's Budget Request. These changes include data collection associated with the Federal Enterprise Architecture (FEA), Project Management Qualification Status, Investment Certification and Accreditation Status, and Mission Area/MA Domain[1]/Domain Package reporting. FEA, PM, and C&A information will be forwarded as part of exhibit 53. Components will complete the exhibit at attachment F vice using the Initiative Registration process within SNaP-IT for collection of this information. A spreadsheet that contains pre-populated information for each initiative can be downloaded from SNaP-IT in Documents/Controlled Documents/Additional Ex53 Data Collection Templates. Components are to email one consolidated spreadsheet to Mr. Craig Garant at craig.garant@osd.mil NLT COB August 5, 2005 (Close of Initiative Open Season). Component submissions are to be in Microsoft Excel format and use the naming convention [FY07BES Data Collection - Attachment E - Component_Title.xls].

2. Project Management Qualification Status:
    a. For **Major Investments**
        1. All Exhibit 300s should have a PM assigned.
        2. Agencies should use section I.D of budget exhibit 300 to identify the required PM skill level for each investment (e.g., does the project require a skill level 1, 2, or 3 for the assigned PM)., and whether the

[1] DoD Core Business Missions for the Business Mission Area

assigned PM's qualifications have been validated against the CIO Council guidance.

Per CIO Matrix:

Level 1 - Projects with low-to-moderate complexity and risk (example: Bureau-level (translation - Component Level) projects such as stand-alone information systems with low-to-moderate complexity.

Level 2 - Projects with high complexity and/or risk which are critical to the mission of the organization. Example: 1) Projects that are part of a portfolio or projects/systems that impact each other and/or impact mission activities; 2) Department-wide proejcts that impact cross-organizational missions, such as an agency-wide integration that includes large scale Enterprise Resource Planning.

Level 3 - Projects with high complexity and/or risk, and have government-wide impact. Example: 1) Government-wide initiative, Egov or PMA; High interest projects with Congress, GAO, OMB or the general public; 3) Cross-cutting initiative; Homeland Security.

"Validated"- PM has met the appropriate training and experience requirements for the system/project managed (i.e., the level number (1,2 or 3) of the Project Manager is equal or higher than the level of the system/initiative managed).

"Validated with exception" – PM has not met all of the appropriate training and experience requirements, however, warrants validation with exception (and is qualified) based on demonstrated successful performance on the job.

"In the Process of Being Validated" – PM has not fully met appropriate training requirements, however, actions are being taken to address the requirement.

3. All Exhibit 300 PMs should be Qualification Status 1 (validated or validated with exception) or 2 (in the process of being validated).
4. Do not use Qualification Status 3 or 6; Qualification Status 5 should only be used if current position is vacant, with explanation provided in section I.D. of Exhibit 300.

b. For **Non-major Investments.** Qualification Status should ideally be 1 or 2 if the project/system rates a PM, however, given that this is a new reporting requirement, it is acceptable to use Qualification Status 4 if time constraints preclude gathering sufficient data on which to make a validation decision. Additionally, if Components have non-acquisition initiatives that do not

require a PM, use Qualification Status 5. *Neither 3 nor 6 should be used for <u>any</u> investment initiative Qualification Status.*

3. Investment Certification and Accreditation Status: For those initiatives that do not involve systems and therefore do not require Certification and Accreditation, components are to leave the C&A field blank.

<u>Exhibit 300</u>

1. The following programs must identify in section f.1 that they are a part of a PARTed Program (entitled: **Communications Infrastructure**):

0392 COMBAT INFORMATION TRANSPORT SYSTEM
0595 DEFENSE INFORMATION SYSTEM NETWORK
2180 INSTALLATION INFORMATION INFRASTRUCTURE MODERNIZATION PROGRAM
6310 NAVY MARINE CORPS INTRANET (NMCI)
6462 DOD TELEPORT

2. PY through BY+3 resources will be populated from the resource entries in SNaP-IT. The "BY-1 and Earlier" and the "BY+4 and Beyond" columns of the Summary of Spending table are to be completed within the exhibit 300 table directly.

3. New Exhibit 300 for "Key Management Infrastructure" will be completed by NSA and will only be comprised of efforts within NSA.

4. New Exhibit 300 for "Public Key Infrastructure" (PKI), Initiative #6456, will be completed by DISA and will focus primarily on the DISA and NSA efforts.

5. "**I.B. Justification (All Assets)**".

"1. How does this investment support your agency's mission and strategic goals and objectives?"

The DoD Mission: The purpose of the U.S. Armed Forces is to protect and advance U.S. national interests and, if deterrence fails, to decisively defeat threats to those interests (QDR, Sept 30, 2001).

The Department's Transformation Goals: To keep the peace and defend freedom in the 21st century our defense strategy and force structure must be focused on achieving six transformational goals:

- protect the U.S. homeland and critical bases of operations.
- project and sustain power in distant theaters.
- deny our enemies sanctuary.
- leverage information technology.

- improve and protect information operations.
- enhance space operations.

Source: *Points from Secretary Rumsfeld's speech at the National Defense University on January 31, 2002)*

The Department's Strategic Objectives: The *National Defense Strategy* outlines an active, layered approach to the defense of the nation and its interests. It seeks to create conditions conducive to respect for the sovereignty of nations and a secure international order favorable to freedom, democracy, and economic opportunity. This strategy promotes close cooperation with others around the world who are committed to these goals. The Department's strategic objectives:

- Secure the United States from direct attack. We will give top priority to dissuading, deterring, and defeating those who seek to harm the United States directly, especially extremist enemies with weapons of mass destruction (WMD).
- Secure strategic access and retain global freedom of action. We will promote the security, prosperity, and freedom of action of the United States and its partners by securing access to key regions, lines of communication, and the global commons.
- Strengthen alliances and partnerships. We will expand the community of nations that share principles and interests with us. We will help partners increase their capacity to defend themselves and collectively meet challenges to our common interests.
- Establish favorable security conditions. Working with others in the U.S. Government, we will create conditions for a favorable international system by honoring our security commitments and working with other nations to bring about a common appreciation of threats; the steps required to protect against these threats; and a broad, secure, and lasting peace.

Source: *The National Defense Strategy of the United States of America*, March 2005

Describe how your investment supports the Department's mission, strategic goals and objectives. If your investment does not support the Department's mission and strategic goals and objectives, then answer "No" and explain why the investment is necessary.

"2. How does the investment support the strategic goals from the President's Management Agenda?**"**

In July 2001, the President directed Cabinet Secretaries and agency heads to designate a "chief operating officer" to have responsibility for day-to-day operations of departments and agencies. Typically, the department's No. 2

official, its "chief operating officer", has agency-wide authority and reports directly to the agency head. The assignment places "management" with Presidential appointed officials, primarily at the deputy secretary level, where policy and management meet.

There are the five government-wide goals in the Presidents Management Agenda:

- Strategic Management of Human Capital,
- Competitive Sourcing,
- Improved Financial Performance,
- Expanded Electronic Government, and
- Budget and Performance Integration

In addition to the five government-wide goals, there are nine agency-specific reforms:

- Faith-based and Community Initiatives,
- Privatization of Military Housing,
- Better Research and Development Investment Criteria,
- Elimination of Fraud and Error in Student Aid Programs and Deficiencies in Financial Management,
- Housing and Urban Development Management and Performance,
- Broadened Health Insurance Coverage through State Initiatives,
- A "Right-Sized" Overseas Presence,
- Reform of Food Aid Programs,
- Coordination of Veteran's Affairs and Defense Programs and Systems.

Describe how your investment supports the President's strategic goals and objectives. If your investment does not support the President's goals and objectives, then state "No" and explain why the investment is necessary.

"8. How does this investment reduce cost and improve efficiencies?"

If the investment does not reduce cost and improve efficiencies, then answer "This investment does not reduce cost and improve efficiencies." Explain why. If the investment does reduce cost and improve efficiencies, then answer "This investment reduces cost and improves efficiencies." This determination should be linked with the Performance Reference Model, Table 2 entry. For example, if the investment is to reduce cost and improve efficiencies, then a measurement indicator should be established to measure these attributes and show it in "Measurement Indicator" column.

6. "**I.C. Performance Goals and Measures (All Assets)**". Table 2 will be used for all projects. There should be at least one Measurement Indicator in each of the four

Measurement Areas (for each fiscal year). A generic sample of Table 2 entries can be located at attachment G.

Examine the Department's annual performance plan: "**2004 Secretary of Defense Annual Report to the President and the Congress"** http://www.dod.mil/execsec/adr2004/adr2004_toc.html to determine whether your investment is associated with the key dimensions of risk that enables the Secretary to evaluate the size, shape, posture, commitment, and management of our armed forces relative to the objectives of the *National Defense Strategy*. Determine whether your investment contributes to the performance being tracked. Select as appropriate the Measurement Area, Measurement Category and Measurement Indicator that is supported by your investment and record it in Table 2 of Section 1.C according to OMB instructions on the use of Table 2. Additional information about aligning the investment to the DoD's mission and strategic goals can be found in the DoD Enterprise Architecture Performance Reference Model located at the ASD(NII) public Web site, http://www.dod.mil/nii, click on "Others" to locate the DoD EA RMs.

7. "**I.D. Project Management (Investment Management)**". The Project (investment) manager of a project is generally the Program Manager or funding sponsor (if not the program manager). The Sponsor/Owner is generally the organizational entity (e.g. Program Executive Officer, Assistant Secretary of Defense). For acquisition projects it would be the program manager, for projects in sustainment, it would be the functional manager.

Project Management Qualification Status, new to EX 53, means the qualification status of the investment's project manager (PM), as issued in OMB PM Guidance **M-04-19** (can be downloaded from SNaP-IT at Public Documents/Miscellaneous/OMB-CIO Council PM Qualifications Guidance). Ensure that your discussion documents your PM qualification status listed in the EX 53. Discussion should also include the following:

1. IT Project Manager/System Levels
   - Level 1: Manage a project within a division, bureau or agency. Projects are low-to-moderate complexity and risk.
   - Level 2: Manage projects with high complexity and/or risk that are critical to the mission of the organization.
   - Level 3: Lead large, inter-governmental or Government-wide complex, high risk/complexity IT project (E-Gov or President's Mgmt Agenda initiative, mission critical function, or high interest project).
2. DAWIA Level
3. DAWIA Career Field
4. Any other Certificate program – e.g. IRMC, AMP, CIO, PMI, etc.

Question I.D.2 should be answered by providing the name of the contracting officer(s). If your initiative utilizes multiple contracting agencies then the following is an example you could use in response to the question:

No single contracting officer provides all support to the Programs. Contracting Officers from many agencies, e.g., Defense Contracting Command - Washington (DCC-W), Veterans Affairs North Texas Health Care System (VANTHCS), US Army Medical Research Acquisition Activity (USAMRAA), Department of Interior (DOI) National Business Center, and General Services Administration (GSA) support this project.

8. "**I.F Risk Inventory and Assessment (All Assets)**". The Current Status column now requires to you *"list the milestones remaining to mitigate the risk"*, therefore, in addition to the stoplight listed below you must include the remaining milestones. The Current Status scoring code:

'Green' (i.e., on-track);
'Yellow But Improving';
'Yellow' (i.e., potential or actual problem);
'Red But Improving';
'Red' (i.e., major weakness);
'Not Applicable'

9. "**II.A. Enterprise Architecture (EA)**". The FY07 Budget Formulation FEA Consolidated Reference Model Document can be downloaded from SNaP-IT at Public Documents/PBR07-11.

The Clinger-Cohen Act requires agencies to have an Enterprise architecture that describes the current and future architecture for the agencies. The business case needs to demonstrate how the investment conforms to the enterprise architecture and what the implications are for the business and data layers of the architecture. OMB has directed that funding for new initiatives not be provided unless identified in the Agency enterprise architecture.

II.A.1 Business

A. Is this investment identified in your agency's enterprise architecture? If not, why?

Authors should answer "Yes" if their investment aligns with one of the Mission Areas in the DoD EA RMs and is included in SNAP-IT. The mission areas are the Warfighter, Business, Intelligence, and Enterprise Information Environment.

A.1. Will this investment be consistent with your agency's target architecture?

The target architecture is the GIG Architecture Version 2.0 which establishes the target architecture and is synonymous with the Net-centric architecture. Answer should be "Yes". If not explain why not.

B. Was this investment approved through the EA Review committee at your agency?

The GIG Architecture Version 2.0 and resulting Net-centric target was approved by the DoD CIO Executive Board. If your investment is related to advancing the target architecture, then answer "Yes". The responsibility for ensuring whether an investment may go forward has been delegated. For example, IT investments that have been certified as compliant with the DoD Business Enterprise Architecture (BEA) IAW the NDAA certification process should answer "Yes".

While not all investments are governed by a structure as formal as that prescribed by the NDAA certification process the management functions, however, of such a committee are distributed among various organizations and processes within the DoD.

The purpose of an EA Review committee is to ensure that each proposed IT investment:

- Is aligned with the strategic goals, objectives, and priorities of the organization;
- Has system requirements that address critical organizational needs;
- Supports organizational processes that have been clearly defined and "reengineered" to make them more efficient/effective;
- Will be interoperable with the rest of the systems that make up the enterprise architecture
- Will conform to the technical standards established by the organization's enterprise technical architecture

To answer "Yes" if not NDAA certified, programs should:

(1) Have an approved Operational/Capability Requirements Document (or some other formal requirements document that was approved by an organization outside the program office)
(2) Comply with the technical standards documented in the DoD IT Standards Registry (DISR) (available at http://disronline.disa.mil/)
(3) Have an approved Information Support Plan (ISP – formerly called a C4ISP) or have one in development
(4) Have an approved Certificate of Networthiness (CoN) or Certificate to Operate (CtO) or have one in development.

C. What are the major process simplification/reengineering/design projects that are required as part of this IT investment?

This question focuses on changes to the processes supported by the investment, not the investment itself. Programs should identify and describe, as appropriate, any ongoing Business Process Reengineering (BPR) performed in conjunction with the program, and/or any other major changes to the way the users perform their activities as a result of the investment. If no processes were changed, then state: *No major process simplification/reengineering/design projects were required as part of this IT investment.*

D. What are the major organization restructuring, training, and change management projects that are required?

This question focuses on changes to the organization and its personnel as a result of the investment, not the investment itself. Programs should identify and describe any restructuring, training, and/or change management projects required to support their program. Examples would include: a reduction in the number of people required to perform an activity/process supported by the investment due to automation; retraining of users due to a major change in the process or the system supporting the process; or a reorganization of the receiving activity in conjunction with fielding of the investment.

If no major organization restructuring, training, and change management projects were required, then state: *No major organization restructuring, training, and change management projects were required as part of this IT investment.*

E. The FEA BRM is available in the Consolidated Reference Model Document. This document lists all of the high level activities performed by the federal government. It consists of 4 "Business Areas" that are broken into 39 "Lines of Business (LOB)" and further broken into 163 "Sub-functions". The BRM is organized along functional lines – not organizational lines. The intent of this question is to help identify similar IT projects across the federal government, which might be candidates for consolidation, reuse, or divestiture.

Although there is a "Defense and National Security" LOB, programs should not limit themselves to only this category. Programs should review the entire BRM and select a primary and the no more than 3 non-primary Sub-Functions (and associated LOB) that their investment DIRECTLY supports. The primary LOB and Sub-function are reflected in the Report ID number and the Section 53 report and should not be listed in the table above. No more than 3 non-primary should be listed in the table.

Make sure that one of your non-primary mappings is a "Mode of Delivery" LOB/sub-function - such as "Direct Services for Citizens/Military Operations" if your primary BRM mapping is a "Services for Citizens" LOB/Sub-function.

Also, contrary to its title, the Lines of Business and Sub-functions that fall under the "Services to Citizens" Business Area also apply to internal DoD citizens as well – not just the general public.

II.A.3. Applications, Components, and Technology

A. For more information on the SRM, see the Consolidated Reference Model Document. However a discussion of the service component concept is appropriate for understanding to move from the legacy environment of today to service component of the future.

The Service Component Reference Model (SRM) identifies a broad variety of different types of "components". Components represent modular functionality or capability that enables some aspect of the business process or the business process itself. Component is defined as *"a self contained business process or service with predetermined functionality that may be exposed through a business or technology interface."* Components vary in granularity from

- Federated Component. A set of cooperating system-level components federated to resolve the business need of multiple end users often belonging to different organizations.
- Business Component System. A set of cooperating business components assembled together to deliver a solution to a business problem.
- Business Component. Represents the implementation of an autonomous business concept or business process. It consists of all the technology elements (i.e., software, hardware, data) necessary to express, implement, and deploy a given business concept as an autonomous, reusable element of a large information system. It is a unifying concept across the development lifecycle and the distribution tiers.
- Distributed Component. The lowest level of component granularity. It is a software element that can be called at run-time with a clear interface and a clear separation between interface and implementation. It is autonomously deployable.

The SRM lists 171 "components" organized into 30 "Service Types" and 7 "Service Domains". The intent of this question is to help identify similar IT projects across the federal government which might be candidates for consolidation, reuse, or divestiture.

CIR authors should review the entire SRM and identify at least **1** and no more than **5** components (and associated "Service Type" and "Service Domain") that best describe the functionality provided by their investment. Recognize upfront that some of the components share similar functionality – so select those that best describe your investment's functionality, capabilities, and primary purpose.

In the "Relation to the SRM" field provide no more than a sentence description of how your investment relates to the listed service component. Use the description of the SRM component from the Consolidated Reference Model Document and tailor it to your application.

Given the Department is transitioning to a net-centric environment to enable a service oriented architecture the following guidance is provided regarding the SRM table to be completed in your CIR. Several examples are provided in the following Tables:

Table 1 provides examples of the type of Component that has a tailored Component Description. The Component is of a particular Service Domain, and Service Type but the description must be tailored to reflect the specific use of the Component. For example in the Table 1, the tailored description reads "*The xxx system allows access to logistics related data and information for use by logisticians" vs* the SRM description of "*Support the use of documents and data in a multi-user environment for use by an organization and its stakeholders"*. The author can see that the OMB SRM definition has been slightly tailored.

Table 1 (Itemized list of components – with tailored Component Description):

Relation to SRM (i.e. Component Description)	Service Domain	Service Type	Component	New Component? (Yes or No)
The xxx system allows access to logistics related data and information for use by logisticians	*Digital Asset Services*	*Knowledge Management*	*Information Retrieval*	*No*
The xxx system allows users to share documents and data in a multi-user environment	*Digital Asset Services*	*Knowledge Management*	*Information Sharing*	*No*

Table 2 provides an example of the type of Component that provides most or all of the functionality with a "Service Type". The Component description must reflect "all" or "most" which ever it is. See the Consolidated Reference Model for the full list of Service Components that make up the "Service Type" named "*Human Capital/Workforce Management"*.

Table 2 (System implements all or most of the components within a "Service Type"):

Relation to SRM (i.e. Component Description)	Service Domain	Service Type	Component	New Component? (Yes or No)
The xxx system provides all (most) of the capabilities reflected in the Human Capital/Workforce Management Service Type by providing capabilities that support the planning and supervision of personnel within the organization.	*Back Office Services*	*Human Capital/Workforce Management*	*Skills Management*	*No*

If the components you identify are not autonomous, reusable elements that are separately field able, accessible or sharable by users (i.e. they are an integral part of your system) then you should define a "Composite New Component" that will be used when you fill out the Technical Reference Model (TRM) table in question II.A.3.C (below). The SRM table entries should look as shown in Table 3. An example is given in Table 3.a. Further, you only identify "New Component" (rather than "Composite New Component") when the component is autonomous, made up of reusable elements that are separately field able, accessible or sharable by users. An example of a "New Component" is shown in Table 4.

Table 3. "Composite New Component" column-by-column instructions:

Relation to SRM (i.e. Component Description)	Service Domain	Service Type	Component	New Component? (Yes or No)
*List "***System Acronym".** *State "***A composite component that integrates all of the functionality described by the SRM components listed for this IT investment."**	*Select the Service Domain associated with the Service Type selected.*	*Select the appropriate Service Type (should be same as your primary SRM component)*	*(Leave Blank)*	*State* **Yes**

Table 3.a. Example of a "Composite New Component" for the Financial Information Resource System (FIRST):

Relation to SRM (i.e. Component Description)	Service Domain	Service Type	Component	New Component? (Yes or No)
FIRST. A composite component that integrates all of the functionality described by the SRM components listed for this IT investment.	Back Office Services	Financial Management		*State* **Yes**

Table 4. Example of a "New Component" (not "Composite New Composite") that aligns directly with the FEA SRM, for example):

Relation to SRM (i.e. Component Description)	Service Domain	Service Type	Component	New Component? (Yes or No)
XYZ, Data Warehouse supports the archiving and storage of large volumes of data	*Back Office Services*	*Data Management*		*State* **Yes**

C. The Technical Reference Model (TRM) identifies and categorizes a broad variety of technologies and technical standards that are used or implemented by systems to provide the functionality required by the user. The TRM lists 50 "Service Standards" organized into 17 "Service Categories" and 4 "Service Areas".

If you identified a new "composite" component in the SRM table above - then you should review the entire TRM and identify the Service Standards (and associated "Service Category" and "Service Area") that best describe the primary technologies used to implement their new "composite" component.

OMB is using the Service Specification column to identify Commercial Off-the-Shelf (COTS) products that might be candidates for inclusion in federal SMARTBUY government-wide software contracts (see http://www.cio.gov/index.cfm?function=documents&section=smartbuy for more information).

CIR preparers should identify, where possible, the specific COTS products used to implement each Service Standard listed in the TRM table. Do not list hardware products or custom developed products; only list a COTS product once, associated with the Service Standard.

If you did not define a new "composite" component in the SRM table above, or your initiative includes SRM components that are autonomous, reusable elements, then you should list each SRM component and its associated Service Standards (and associated Service Category and Service Area) and, where possible, the COTS product used.

D. Will the application leverage existing components and/or applications across the Government (i.e., FirstGov, Pay.Gov, etc). If so, please describe.

OMB is very interested in examples of sharing/leveraging of IT investments across the government (cross-DoD doesn't count). If your program currently uses or plans to use applications or components developed or operated by another agency outside the DoD then state as such and describe the component/application and which agency is providing it.

If your investment does not leverage components/application external to DoD then state: *The xxx investment does not use any existing components and/or applications external to the DoD.*

E. If the investment was identified in the screening questions as a FM system, the author needs to determine the mapping requested.

10. Section II.B. Security and Privacy. Security is a key focus area for OMB. The following additional information is provided to assist with completion of your submission.

For reporting, "Does the investment have an up-to-date Security Plan that meets OMB Policy/NIST Guidelines?"

The System Security Authorization Agreement (SSAA) is the security plan in accordance with DITSCAP (DoDI 5200.40 and DoD 8510.1-M). Provide date of plan.

Note: Reference DoD 8510.1-M, (C2.1.1.5.). DITSCAP uses a single document approach. All the information relevant to the C&A is collected into the one document, the Systems Security Authorization Agreement (SSAA). The SSAA is designed to fulfill the requirements of OMB Circular No. A-130 (reference (d)) for a security plan and to meet all the needs for C&A support documentation.

For reporting, "Has the investment been certified and accredited (C&A)?

If investment has an Authority to Operate (ATO) answer should be: **Yes, ATO, Date of ATO**. State methodology is DoD Information Technology Security Certification and Accreditation Process (DITSCAP). If investment has an Interim Authority to Operate (IATO), answer should be: **Yes, IATO, Date of IATO.**

Note: Certification and accreditation refers to full C&A and does not mean interim authority to operate.

Note: C&As are to be performed prior to the system becoming operational. If the system(s) described in the business care are in the initial concept of development phase, the agency needs to state that a C&A will be conducted prior to the system becoming operational. **Please include the planned date for any system not yet operational.**

For reporting, "Have the management, operational, and technical security controls been tested for effectiveness?" "When was most recent tests performed?"

SSAA should document the initial and may document subsequent testing and validation. FISMA now requires evaluation annually. Such testing need not be documented in the SSAA. The DoD 8500.2 controls are the basis for management, operational and technical controls being tested. The OMB answer they are looking for is "Yes", and date of the most recent tests performed.

For reporting, "Have all system users been appropriately trained in the past year, including rules of behavior and consequences?"

State yes or no. Training required by DoDD 8500.1/DoDI 8500.2/DoDI 5200.40.

For reporting, "How has Incident handling capability been incorporated into the system or investment, including intrusion detection monitoring and audit log reviews? Are incidents reported to DHS' US CERT?

SSAA documents incident handling; DoD systems reported to Component CERTS, DoD CERT/JTF-CNO. Yes, DoD CERT forwards incidents to DHS' US CERT as appropriate.

For reporting, "Is the system operated by contractors either on-site or at a contractor facility?"

If applicable, should be documented in SSAA. Answer all the questions.

For reporting, "How does agency ensure effective use of security controls and authentication tools to protect privacy for systems that promote/permit public access?"

Confidentiality controls specified in DoDI 8500.2 for publicly released information.

For reporting, "How does agency ensure handling of personal information is consistent with relevant gov't-wide and agency policies?"

Confidentiality controls specified in DoDI 8500.2 for sensitive information for Privacy Act, proprietary, FOUO, etc. If applicable, state if investment does not handle personal information.

2005 National Defense Authorization Act (NDAA) Section 332 § 2222 (h)

1. Section 332 § 2222 (h) of the 2005 National Defense Authorization Act (NDAA) requires the Secretary of Defense submit, to Congress, budget information for defense business systems. In order to meet these requirements, "defense business systems" will be reported separately within the Information Technology (IT) Budget for FY2007 and fiscal years thereafter. Defense business systems are defined within Sec. 332 § 2222 (j)(2). Guidelines for determining what "is" and what "is not" a defense business system are provided at attachment H and are consistent with DoD Directive 8000.1 (Management of DoD Information Resources and Information Technology) and department guidelines utilized by DITPR, DoD IT Registry and the IRB process.

2. Defense business systems must be included within the IT Budget at the system level, not as system of systems, family of systems, or bundle of systems (i.e., Defense Business System = Initiative).

Attachment A

List of Initiatives Requiring an EX300 for FY07

	In_num	Acronym	IntTtl	Component
1	0392	CITS	COMBAT INFORMATION TRANSPORT SYSTEM	Air Force
2	1826	ISPAN	INTEGRATED STRATEGIC PLANNING AND ANALYSIS NETWORK	Air Force
3	1911	TBMCS	THEATER BATTLE MANAGEMENT CORE SYSTEMS	Air Force
4	1912	TDC	THEATER DEPLOYABLE COMMUNICATIONS	Air Force
5	5069	GCSS-AF	GLOBAL COMBAT SUPPORT SYSTEM - AIR FORCE	Air Force
6	6170	AFMSS	AIR FORCE MISSION SUPPORT SYSTEM	Air Force
7	6189	JPALS	JOINT PRECISION APPROACH AND LANDING SYSTEM	Air Force
8	6197	BCS-M	BATTLE CONTROL SYSTEM - MOBILE	Air Force
9	6460	AMC C2	MOBILITY COMMAND AND CONTROL	Air Force
10	6524	AMF JTRS	AIRBORNE AND MARITIME/FIXED STATION JOINT TACTICAL RADIO SYSTEM	Air Force
11		AOC-WS	Air Operations Center - Weapon System	Air Force
12	6320	CMC/TW-AA	Cheyenne Mountain Complex/Tactical Warning-Attack Assessment	Air Force
13	0483	ECSS	Expeditionary Combat Support System	Air Force
14	0043	A2C2S	ARMY AIRBORNE COMMAND AND CONTROL SYSTEM	Army
15	0048	TOCS	TACTICAL OPERATIONS CENTERS	Army
16	0145	DMS-A	DEFENSE MESSAGE SERVICE - ARMY	Army
17	0314	GFEBS	GENERAL FUND ENTERPRISE BUSINESS SYSTEM	Army
18	0688	DLS	DISTRIBUTED LEARNING SYSTEM	Army
19	1499	PENREN	PENTAGON RENOVATION-INFORMATION MANAGEMENT & TELECOMMUNICATIONS	Army
20	1640	RCAS	RESERVE COMPONENT AUTOMATION SYSTEM	Army
21	1935	TC-AIMS II	TRANSPORTATION COORDINATORS' AUTOMATED INFORMATION FOR MOVEMENTS SYSTEM II	Army
22	2166	AFATDS	ADVANCED FIELD ARTILLERY TACTICAL DATA SYSTEM	Army
23	2180	I3MP	INSTALLATION INFORMATION INFRASTRUCTURE MODERNIZATION PROGRAM	Army
24	2212	FAADC2	FORWARD AREA AIR DEFENSE COMMAND AND CONTROL SYSTEM	Army
25	2213	MCS	MANEUVER CONTROL SYSTEM	Army
26	5047	WARSIM2000	WARFIGHTER SIMULATION 2000	Army
27	5070	GCSS - A	GLOBAL COMBAT SUPPORT SYSTEM - ARMY	Army
28	6040	ARISS	ARMY RECRUITING INFORMATION SUPPORT SYSTEM	Army
29	6185	FBCB2	FORCE XXI BATTLE COMMAND BRIGADE AND BELOW	Army
30	6190	JTRS-Cluster 1	JOINT TACTICAL RADIO SYSTEM - CLUSTER 1	Army
31	6198	WIN-T	WARFIGHTER INFORMATION NETWORK-TACTICAL	Army
32	6298	LMP	LOGISTICS MODERNIZATION PROGRAM	Army

33	6306	DTT	DISTRIBUTIVE TRAINING TECHNOLOGY	Army
34	6430	KM	KNOWLEDGE MANAGEMENT	Army
35	6491	GCCS-A	GLOBAL COMMAND AND CONTROL SYSTEM - ARMY	Army
36	6506	SMART-T	SECURE MOBILE ANTI-JAM RELIABLE TACTICAL-TERMINAL	Army
37	6587	JTRS(JPO)	JOINT TACTICAL RADIO SYSTEM (JOINT PROGRAM OFFICE)	Army
38	6597	C2 Facilit	STRATEGIC COMMAND AND CONTROL FACILITIES	Army
39	6963	GuardNet	GUARDNET XXI, THE ARMY NATIONAL GUARD'S WIDE AREA NETWORK	Army
40	0342	JTRS C5	Joint Tactical Radio Ssystem - Cluster 5	Army
41	1794	SPS	STANDARD PROCUREMENT SYSTEM	DCMA
42	0277	CARTS	COMMISSARY ADVANCED RESALE TRANSACTION SYSTEM	DeCA
43	0138	FCP	FORWARD COMPATIBLE PAYROLL	DFAS
44	0573	DCPDS	DEFENSE CIVILIAN PERSONNEL DATA SYSTEM	DHRA
45	4035	DEERS	DEFENSE ENROLLMENT ELIGIBILITY REPORTING SYSTEM	DHRA
46	6521	DIMHRS	DEFENSE INTEGRATED MILITARY HUMAN RESOURCES SYSTEM	DHRA
47	0595	DISN	DEFENSE INFORMATION SYSTEM NETWORK	DISA
48	0615	DMS	DEFENSE MESSAGE SYSTEM	DISA
49	0881	GCCS-J	GLOBAL COMMAND AND CONTROL SYSTEM- JOINT	DISA
50	0882	GCSS	GLOBAL COMBAT SUPPORT SYSTEM-COCOM-JTF	DISA
51	5061	DECC	DEFENSE ENTERPRISE COMPUTING CENTERS	DISA
52	6456	PKI	Public Key Infrastructure	DISA
53	6462	Teleport	DOD TELEPORT	DISA
54	6965	NCES	NET CENTRIC ENTERPRISE SERVICES	DISA
55	0344	EDC	Enterprise Data Center	DLA
56	5090	BSM	DLA BUSINESS SYSTEMS MODERNIZATION	DLA
57	0594	DISS	Defense Information System for Security	DSS
58	0155	GCSS- USMC	GLOBAL COMBAT SUPPORT SYSTEM - MARINE CORPS	NAVY
59	0186	NAVY ERP	NAVY ENTERPRISE RESOURCE PLANNING (ERP)	NAVY
60	1372	NTCSS	NAVY TACTICAL COMMAND SUPPORT SYSTEM	NAVY
61	6046	GCCS-M	GLOBAL COMMAND AND CONTROL SYSTEM - MARITIME	NAVY
62	6310	NMCI	NAVY MARINE CORPS INTRANET (NMCI)	NAVY
63	6434	NPM-ERP	NAVAIR PROGRAM MANAGEMENT- ENTERPRISE RESOURCE PLANNING	NAVY
64	6555	DJC2	DEPLOYABLE JOINT COMMAND AND CONTROL	NAVY
65		KMI	Key Management Infrastructure	NSA
66	6312	DTS	DEFENSE TRAVEL SYSTEM	OSD
67	6497	BMMP	BUSINESS MANAGEMENT MODERNIZATION PROGRAM	OSD
68	0332	MCPR	MILITARY COMPUTER-BASED PATIENT RECORD (includes #0435 and 0049)	TMA
69	0510	EI/DS	EXECUTIVE INFORMATION/DECISION SUPPORT	TMA
70	0613	DMLSS	DEFENSE MEDICAL LOGISITICS STANDARD SYSTEM	TMA
71	1913	TMIP	THEATER MEDICAL INFORMATION PROGRAM	TMA
72	6594	JPEHR	JOINT PLAN FOR THE ELECTRONIC HEALTH RECORD	TMA

73	6596	TIMPO	TRI-SERVICE INFRASTRUCTURE MANAGEMENT PROGRAM	TMA
74	0178	DEAMS	DEFENSE ENTERPRISE ACCOUNTING AND MANAGEMENT SYSTEM	TRANSCOM
75	0884	GDSS	GLOBAL DECISION SUPPORT SYSTEM	TRANSCOM
76	6487	GTN 21	GLOBAL TRANSPORTATION NETWORK 21	TRANSCOM

Attachment B

MILDEP and Agency Consolidated Business Case for Infrastructure

Date of this Submission
MILDEP/Agency Name

Initiatives Covered by this business case:

(Initiatives comprising of the BES06 Communications and Computing Infrastructure GIG Category)

Initiative Number	Initiative Name	Total Resources PY	Total Resources CY	Total Resources BY	EX300 submitted? (Y/N)

I. A. Description

1. Provide a brief description of this capability and its status through your capital planning and investment control (CPIC) or capital programming "control" review for the current cycle.
2. What assumptions are made about this capability and why?

I.B. Justification (All Assets)

1. How does this capability support your MILDEP/agency's mission and strategic goals and objectives?
2. Are there any alternative sources in the public or private sectors that could perform these functions?
3. If so, explain why your MILDEP/agency did not select one of these alternatives.

I.C. Performance Goals and Measures (All Assets)

1. How does the governance process meet the needs of the MILDEP/agency?
2. How does the governance process measure performance?
3. Describe the process to update guidance or take action if the MILDEP/agency determines that the performance is not being met?

I.D. Enterprise Architecture

1. Describe the MILDEP/agency supports the business aspect of the Net Centric Operations & Warfare reference model?

I.E. Security and Privacy

1. Describe the governance process that ensures information and computer security.
2. Identify any associated information assurance efforts in support of (but may not be limited to) the Communications and Computing Infrastructure GIG Category.
3. How does the governance process address and ensure initiatives have been certified and accredited (C&A)?

Attachment C

MILDEP Enterprise Architecture Discussion

Date of this Submission
MILDEP/Agency Name

Initiatives Covered by this discussion:

Initiative Number	Initiative Name	Total Resources PY	Total Resources CY	Total Resources BY

1. Provide a brief description of the MILDEP Enterprise Architecture.
2. Provide a description of the maturity level of your Enterprise Architecture.
3. How does the MILDEP Enterprise Architecture align with OMB EA Assessment version 1.5.
4. What assumptions are used in the development of the MILDEP Enterprise Architecture?
5. What governance process oversees the MILDEP Enterprise Architecture effort?
6. How does the governance process measure compliance?
7. Describe the process to update guidance or take action if the MILDEP Enterprise Architecture requirements are not being met?
8. Identify milestones for success with dates and indicate if you have met these milestones and are on schedule to meet future milestones.

Attachment D

FY07 BMMP Modified Exhibit 300
for (name of DoD Core Business Mission Area)

1. Provide budget table of resources.

	PY-1 and Earlier	PY	CY	BY	BY +1	BY +2	BY +3	BY +4 and Beyond
RDT&E								
O&M								

2. Describe the Core Business Mission Area's goal, objectives, and the performance metrics that will be used to assess progress.

3. How does this investment support the President's Management Agenda, the Core Business Mission Area's mission, strategic goals and objectives?

4. Describe briefly, or attach, the Core Business Mission Area's Implementation Plan. The plan should address, at a minimum, portfolio management and the investment management strategy (certification process).

5. Provide Core Business Mission Area milestones, deliverables, and accomplishments for FY 2006 and FY 2007.

6. Provide a summary table of planned spending by element of expense for FY 2006 and FY 2007.

7. Describe how the Core Business Mission Area aligns with the Business Enterprise Architecture (BEA).

8. Discuss the Core Business Mission Area specific risk as well as the Core Business Mission Area/TSO shared risk and how the risk aligns with the development and implementation of the BEA.

9. Provide a list of all the IT systems within the Core Business Mission Area's Investment Portfolio.

10. Provide summary chart of all systems with available cost data (Table format will be developed to allow extraction from the IT1).

ITMA number	System Title	Acronym	Core Business Mission Area Certified	PY	CY	BY

11. Describe how the Core Business Mission Area intends on collecting system cost data for systems not currently reporting costs.

12. Describe how the Core Business Mission Area plans to ensure all the applicable security requirements are captured in the BEA and in new or modified systems required to adhere to the BEA. How will security related issues be funded?

Attachment E

Sample Format for the Statement of Compliance

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (NETWORKS, INFORMATION AND INTEGRATION)

SUBJECT: Statement of Compliance for the FY 2007 Information Technology/National Security Systems (IT/NSS) President's Budget Submission

The [component] FY 2007 President's Budget Submission for the IT/NSS Exhibits (submitted via the SNaP-IT) are in compliance with Financial Management Regulation, Volume 2B, Chapter 18. The IT/NSS Exhibits are complete; accurately aligned with the [component]'s primary budget, program and acquisition materials; and are consistent with the Clinger-Cohen Act, OMB A-11 and documented exceptions to the circular, DoD CIO budget guidance memorandum, Paperwork Reduction Act and other applicable Acts and requirements.

The POC for the [component] IT/NSS submission is [name], [phone number], [email address].

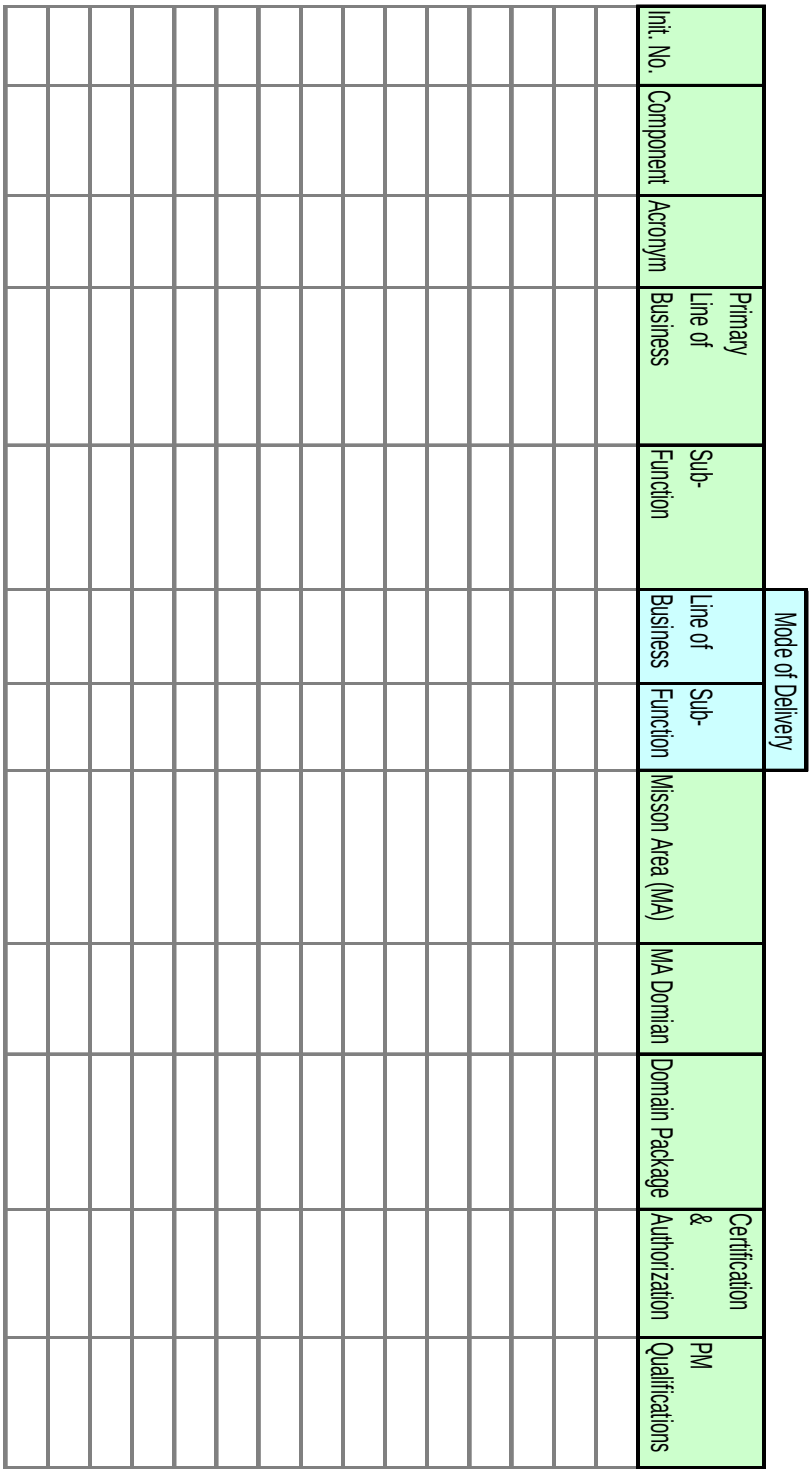
_____ _____

[Component CIO] [Component CFO]

Attachment F

Example of new Exhibit 53 Data Collection Spreadsheet

Component Spreadsheets can be downloaded from SNaP-IT
at Documents/Controlled Documents/Additional Ex53 Data Collection Templates



Attachment G

Example of a DoD Table 2 Exhibit

Project Name –Logistics Support System

Generic Sample IT 300 Section 1C Table 2 Entries
6/10/04

Fiscal Year	**Measurement Area**	**Measurement Category / Indicator Grouping (**in PRM, not IT300)	**Measurement Indicator**	**Baseline**	**Planned Improvements to Baseline**	**Actual Results**
2005	Mission and Business Results	Management of Government Resources - Supply Chain Management / Goods Acquisition	Annual return ratio = price discounts of medical purchases made via electronic commerce / total annual IT initiative program funding.	Baseline before IT investment: Annual return ratio is X:1	Improve the resource efficiency of the MHS by achieving an annual return ratio of Y:1 comparing price discounts of medical purchases made via electronic commerce to total annual IT initiative program funding.	As of 3rd Qtr. 75% of efficiency goal met
2005	Customer Results	Service Accessibility / Automation	The number of logistics managers (measured by sites) who have access to purchasing medical supplies via e-commerce.	Baseline is the number of logistics managers with access to this capability before IT system deployment = 0.	Number of logistics managers scheduled to receive the IT capability by the end of FY05.	Mid-year rate 59%
2005	Processes and Activities	Financial / Costs	The dollar value of supply purchases made via e-commerce.	The baseline is the dollar value of supply purchases made via e-commerce before deployment of the Capability or at a specific point in time = $X.	Increase the efficiency and accuracy of supply product purchases by increasing the dollar value of supply purchases made via e-commerce rather than manually by $Y over baseline.	As of 3rd Qtr X% improve
2005	Technology	Effectiveness / IT Contribution to Process, Customer, or Mission	The number of sites with e-commerce supply purchasing capability	Baseline = # of sites with e-commerce before IT system deployment = 0.	# of sites planned for deployment by end of FY05.	Data Not available yet

Attachment H

Defense Business System
Definition and Guidelines

Definition

The term 'defense business system' means an information system, other than a national security system, operated by, for, or on behalf of the Department of Defense, including financial systems, mixed systems, financial data feeder systems, and information technology and information assurance infrastructure, used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management. (2005 NDAA Sec. 332 § 2222 (j)(2))

Guidelines

Examples of IT systems included in the above definition are:

- DoD-wide, Joint systems
- Federal System used by DoD or supported by DoD
- DoD System used as a Federal System
- Multi-Component System
- Component Standard System
- Major Command Standard System (Echelon 2 or equivalent for Navy and
- Marine Corps)
- Below Major Command System (below Echelon 2 or equivalent for Navy and Marine Corps) (e.g., bridges, uniques used at a single site)
- Data Stores/Data Warehouses
- Enclaves
- Portals (Enterprise)
- Automated Information System (AIS) Application

Examples of IT that **should not** be reported separately in SNaP-IT, but should be included as part of another reported system are:

- Commercial Off-the-Shelf (COTS) Office Automation
- Modules
- Subsystems
- Software Product/Suite
- Automatic Identification Tag
- IT labor skill
- Internal script
- Open Data-Base Connectivity (ODBC) object
- Portals (System specific)